information associated therewith. In some embodiments, the method may also include transmitting a notification to the user device if the identified candidate poses a high risk to the public or is a criminal. In some embodiments, the personal information may include a name of the identified candidate. In some embodiments, the personal information may include a link to an online profile associated with the identified match. In some embodiments, the personal information transmitted to the user device is obtained from a webpage having the highest PageRank value among the webpages containing the personal information.

[0027] In some embodiments, the facial recognition module is operable to: (i) determine a permission of access for the subject to a venue or an account based on the personal information of the identified candidate; (ii) grant the access for the subject if the identified candidate is an authorized user, or deny the access for the subject if the identified candidate is not an authorized user or the candidate matching the captured facial image cannot be identified; and (iii) transmit a message indicative of granting or denying the access to the venue or the account. In some embodiments, the account may be associated with a bank, a financial institute or a credit company.

[0028] In some embodiments, the facial recognition module is operable to provide access to the database to a plurality of users. The plurality users may be located in the same geographic area or associated with the same business type.

[0029] In some embodiments, the facial image data include a second captured facial image of a second subject. In some embodiments, the method includes identifying a relationship between two or more subjects having facial images captured in a single image.

[0030] In another aspect, this disclosure provides a system for verifying an identity of a user. The system includes (i) a facial image processing module operable to transform a captured facial image of the subject to a facial recognition data; and (ii) a facial recognition module operable to: (a) provide a facial image data comprising a captured facial image and a personal identification number of the user; (b) transform the facial image data to facial recognition data; (c) compare the facial recognition data and the personal identification number to reference facial recognition data and reference personal identification numbers associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image and the personal identification number; and (d) upon identification of the candidate, transmit a confirmation to a user device indicating the user is an authorized user.

[0031] The foregoing summary is not intended to define every aspect of the disclosure, and additional aspects are described in other sections, such as the following detailed description. The entire document is intended to be related as a unified disclosure, and it should be understood that all combinations of features described herein are contemplated, even if the combination of features are not found together in the same sentence, or paragraph, or section of this document. Other features and advantages of the invention will become apparent from the following detailed description. It should be understood, however, that the detailed description and the specific examples, while indicating specific embodiments of the disclosure, are given by way of illustration only, because various changes and modifications within the spirit and scope of the disclosure will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0032] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[0033] FIG. **1** shows an example method for providing information about a person based on facial recognition.

[0034] FIG. **2** shows an example process for providing information about a person based on input images.

[0035] FIG. **3** shows an example process for retrieving facial images of a person and other related information from the Internet using a web crawler.

[0036] FIG. **4** shows an example server side implementation of the disclosed methods.

[0037] FIG. **5** shows an example interface of a search application on a mobile device displaying candidate images in the databases matching the captured facial images.

[0038] FIG. **6** shows an example interface showing candidate facial images identified by the search.

[0039] FIG. **7** shows an example interface of a search application on a mobile device displaying information about a person.

[0040] FIG. **8** shows an example neural network implemented for performing facial recognition.

[0041] FIG. **9** shows an example system for implementing the disclosed methods.

[0042] FIG. **10** shows an example computing system for implementing the disclosed methods.

DETAILED DESCRIPTION OF THE INVENTION

[0043] This disclosure provides methods for providing information about a person based on facial recognition and various applications thereof, including face-based check-in, face-based personal identification, face-based identification verification, face-based background checks, facial data collaborative network, correlative face search, and personal face-based identification. The disclosed methods are able to provide accurate information about a person in a real-time manner.

A. Methods and Systems for Obtaining Personal Information Based on Facial Recognition

[0044] In one aspect, this disclosure presents a method for providing information about a subject (e.g., a person, an unknown person, a newly met person, a person with deficient memory, a criminal, an intoxicated person, a drug user, a homeless person). As shown in FIGS. **1** and **2**, the method includes (i) receiving facial image data transmitted from a user device. The facial image data comprises at least a captured facial image of the subject; (ii) transforming the facial image data to facial recognition data; (iii) comparing by a server device the facial recognition data to reference facial recognition data associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image; (iv) upon identification of the candidate matching the captured facial image, retrieving from the database personal information associated with the candidate; and (v) transmitting the personal information to the user device and causing the user device to display the personal information.